United States of America
FEDERAL TRADE COMMISSION
WASHINGTON, DC 20580

Visions and Goals for the Future of IoT in the USA and Globally

Forum Global
The 6th Annual Internet of Things Global Summit
October 4, 2018

Prepared Remarks of Commissioner Rebecca Kelly Slaughter[1]

Thank you to Forum Global for hosting today's important event. It is an honor to be here and I welcome the opportunity to talk about the need for collaborative action across borders to safeguard trust and security in the evolving world of IoT.

The year 2017 brought an estimated 8.4 billion connected things to the world.[2] That number is expected to reach more than 20 billion by 2020.[3] By 2025, the value of these devices, and the ecosystem in which they operate, is estimated to exceed four *trillion* dollars per year and could be as high as 11 trillion.[4] These devices touch all sectors – the military, manufacturing, healthcare, utilities, autos, and of course, the home. Right now, consumer applications are the largest and fastest-growing category of connected devices.[5] But as connected devices increasingly evolve from things *around* us to things *on* us (like my watch) or *in* us (like a connected prosthetic device), the questions of privacy and security with which we are grappling today will take on increasing significance.

I want to use my remarks today to highlight a few issues: first, the importance of building adequate security into IoT devices from the outset; second, some problems the FTC has already

[1] The views expressed in these remarks are my own and do not necessarily reflect the views of the Federal Trade Commission or any other Commissioner.

[2] Press Release, Gartner Inc., *Gartner Says 8.4 Billion Connected "Things" Will Be in Use in 2017, Up 31 Percent From 2016* (Feb. 7, 2017), https://www.gartner.com/newsroom/id/3598917.

[3] *Id.*; Press Release, Juniper Research, *'Internet of Things' Connected Devices to Almost Triple to Over 38 Billion Units by 2020* (July 28, 2015), https://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.

[4] JAMES MANYIKA ET AL., UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS, at 7 (McKinsey Global Institute, 2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world; Hemendra Singh, *Statistics That Prove IoT Will Become Massive from 2018*, Customer Think, (June 18, 2018) *available at* http://customerthink.com/statistics-that-prove-iot-will-become-massive-from-2018/.

[5] JAMES MANYIKA ET AL., UNLOCKING THE POTENTIAL OF THE INTERNET OF THINGS, at n. 2. (McKinsey Global Institute, 2015), https://www.mckinsey.com/business-functions/digital-mckinsey/our-insights/the-internet-of-things-the-value-of-digitizing-the-physical-world

observed with the devices on the marketplace today; and finally, the challenges we as law enforcers have in fulfilling our mission to safeguard consumers in the IoT space.

Let's begin with the good. The innovation in IoT is breathtaking and dizzying with possibilities. I'm an early adopter—if there is a device or an application that can make my life easier, I buy it, I download it, I connect it. I love being able to use my smart watch to pay for things when I inevitably forget my wallet. I have three kids at home and rely on our home assistant to play music, set timers to resolve toy-sharing disputes, and answer profound questions about the demise of the dinosaurs. And if one day I can climb into my minivan and just say "home"—I'm all in.

But we all know the risks posed by connected devices are equally overwhelming. Imagine if someone hacked into my baby monitor and started spying on (or talking to) my baby? What if a company were collecting data on my children's conversations with their connected toys without our knowledge or consent? These aren't random hypotheticals – there has been public reporting on both of these cases.[6]

The hacking of connected devices can cause profoundly personal risks that can literally follow us into our homes. The New York Times reported this summer on a new trend in domestic abuse cases tied to the rise of smart home technology.[7] Internet-connected locks, speakers, thermostats, lights and cameras are now also being used as a means for harassment, monitoring, revenge and control.[8] Imagine trying to break free from an abusive relationship in which your abuser not only imprisons you with physical and emotional intimidation—but also uses your very home to control and undermine you.

These examples point to the bigger issue here: with all of this cutting edge and truly transformative technology comes legitimate concern about the potential risks these devices pose to our safety, our autonomy, and our privacy. The many benefits of IoT devices may be delayed or foreclosed if consumers cannot trust them.

Building that trust starts with two fundamental components: 1) ensuring that the devices are reasonably secure and (2) ensuring that consumers have a clear and accurate picture of what data their devices collect and how that data is stored and used. Poorly designed IoT devices, and poor privacy controls by their manufacturers, jeopardize the privacy of their users and create security risk when attackers attempt to steal data or assume device control.

Our law and our policy discussions often treat the two issues, security and privacy, as distinct. Though difficult to achieve, data security is the easier one to define: how do we keep

---

[6] Ryan Grenoble, *Hacked Baby Monitor Caught Spying On 2-Year-Old Girl In Texas*, Huffington Post, (Aug. 13, 2013), *available at* https://www.huffingtonpost.com/2013/08/13/hacked-baby-monitor-houston-texas-parents_n_3750675.html; Lauren Walker, *Privacy Advocates Call Talking Barbie 'Surveillance Barbie,'* Newsweek, (Mar. 13, 2015), *available at* https://www.newsweek.com/privacy-advocates-want-take-wifi-connected-hello-barbie-offline-313432.

[7] Nellie Bowles, *Thermostats, Locks and Lights: Digital Tools of Domestic Abuse*, NY Times, (June 23, 2018) *available at* https://www.nytimes.com/2018/06/23/technology/smart-home-devices-domestic-abuse.html.

[8] *Id.*

personal data secure and protect against vulnerabilities and unwanted breaches. Privacy is broader and covers questions about consumers' expectations about their personal data, ranging from collection, use, notice, consent, and control, to portability and the right to be forgotten.

But the world of IoT shows us that the line between privacy and security is not bright; it is not even blurry. The two concepts are overlapping and intrinsically related: there can be no assurance of privacy without sound security and most privacy vulnerabilities pose threats to security.

Put another way: we need to think more broadly about how we define data security. How a company collects and uses consumer data and what they tell consumers is not simply a privacy question, it is also a fundamental data security question. If I did not knowingly and willingly give you my data, no amount of cyber hygiene is going to make it "secure"—I have already suffered a breach.

To play out the domestic violence example above: if someone has a connected home alarm, the device manufacturer may well be collecting data on the time and frequency of its use, and sharing or selling that data to a third party. Without adequate privacy policies that address data collection, retention, storage and sharing, an abusive partner could request, buy, or even steal that information, and the user's security is jeopardized. It is important that consumers have meaningful, accurate and understandable information about their device security, as well as data sharing, in order to make informed decisions.

I recognize that transparently presenting consumers with clear information and choices about how their data will be collected and used presents unique challenges in the IoT space—connected devices may have very limited interfaces. But that doesn't mean that connected devices can simply ignore their obligations to build consumer trust through notice and choice.

If anything, the operators of connected devices need to be particularly vigilant about assessing consumer expectations about data collection through a particular device and to stay within those expectations. Consumers might expect that their fitness band is collecting information about their workouts, but not that the data is being sold to marketers and data brokers.

We are at a critical point in the IoT era in terms of getting privacy and security right. At the precipice of exponential growth, we have the opportunity both to thoughtfully develop products that start and stay secure, and to educate consumers early on about how to assess the risks of connected devices, how to choose brands that take privacy and security seriously, and how to maintain device security with patches over the lifespan of the product.

I cannot overstate the importance of getting this right, now. The FTC has continued to observe troubling failures in the marketplace for connected devices—if these failings are not addressed, consumer trust may become compromised to a point where industry struggles to recover.

First, we're continuing to see some very basic failures in product design and pre-release testing. We encourage and expect companies to consider security at the outset, understand well-known vulnerabilities affecting their class of products, and take advantage of low-cost, widely

available measures to protect against them. I'm particularly concerned by easily avoidable problems, for example connected devices that come with default passwords (or don't require a password at all).

Second, while pre-release testing is important, we understand that such testing will not catch all problems. Vulnerabilities will occur that companies may not have foreseen. Companies should make sure that, among other things, they have a process in place to identify and address credible alerts about potential vulnerabilities.

Third, once vulnerabilities are identified after a product's release, there are often challenges in the deployment of updates and patches. In some cases, patches may be available, but not deployed to consumers in a timely manner. In other cases, consumers themselves may be overwhelmed about how to keep up with patches. In yet other cases, companies may not support devices at all after a certain period.

In all of these cases, devices are left compromised. Companies need to think critically from the get-go about how to maintain security over the lifespan of the device and be on the same page with consumers about the length of that lifespan.

So what role does the FTC play in safeguarding consumer trust and security in the IoT?

Perhaps most obviously, we have an important enforcement mission, the exercise of which promotes security and privacy. We've brought a number of cases regarding connected devices, including routers,[9] baby-monitors,[10] smart TVs,[11] and most recently, connected toys.[12] I want to touch briefly on two of these cases.

In our smart TV case, VIZIO, the FTC alleged for the first time that the collection and sharing of contents of communications without consumer consent is unfair. For many of its TVs VIZIO touted its "Smart Interactivity" feature that could offer program suggestions, but failed to inform consumers that the settings also enabled the collection of consumers' viewing data, which was then sold to third parties. The FTC's complaint alleged that VIZIO's data tracking—which occurred without viewers' informed consent—was unfair and deceptive. VIZIO paid 2.2 million to resolve these charges.[13]

---

[9] *ASUSTeK Computer Inc.*, No. C-4587 (July 18, 2016), https://www.ftc.gov/enforcement/cases-proceedings/142-3156/asustek-computer-inc-matter.

[10] *TRENDnet, Inc.*, No. C-4426 (Jan. 16, 2014), https://www.ftc.gov/enforcement/cases-proceedings/122-3090/trendnet-inc-matter.

[11] *FTC v. VIZIO, Inc., and VIZIO Inscape Services, LLC.*, No. 2:17-cv-00758 (D.N.J filed Feb 3, 2017), https://www.ftc.gov/enforcement/cases-proceedings/162-3024/vizio-inc-vizio-inscape-services-llc.

[12] *U.S. v. VTech Electronics Ltd. et al.*, No. 1:18-cv-00114 (N.D. Ill. Jan. 8, 2018), https://www.ftc.gov/enforcement/cases-proceedings/162-3032/vtech-electronics-limited.

[13] Press Release, FTC, *VIZIO to Pay $2.2 Million to FTC, State of New Jersey to Settle Charges It Collected Viewing Histories on 11 Million Smart Televisions without Users' Consent*, (Feb. 6, 2017) https://www.ftc.gov/news-events/press-releases/2017/02/vizio-pay-22-million-ftc-state-new-jersey-settle-charges-it.

In our first connected toy case, V-Tech, the FTC alleged that some of V-Tech's electronic toys collected the personal information of hundreds of thousands of children through a "Kid Connect" app, and that the company failed to provide direct notice to parents or obtain verifiable consent from parents concerning its information collection practices, as required under the Children's Online Privacy Protection Act (COPPA). V-Tech agreed to a settlement order requiring implementation of a comprehensive data security program, subject to independent audits for 20 years, and paid a $650,000 civil penalty.[14]

The FTC's efforts to promote security, however, go beyond enforcement. The Commission also functions as a facilitator of security innovation through research, reports, data analysis, and numerous workshops, symposiums, challenges and conferences. Recent workshop topics include smartTVs,[15] drones,[16] connected cars,[17] and EdTech.[18]

I am proud of the work the FTC is doing in this area, but I also think we should always be looking for ways to be more effective. To begin, IoT devices highlight the limitations posed by our sectoral privacy laws, which put different requirements on the treatment of data depending on the type of data in question. That might have made sense when data was generated and stayed in sector-specific silos.

But my watch here collects and processes myriad different types of highly sensitive data – banking, health, location, and more. Asking device manufacturers to follow different regimes in the treatment of all of those different types of data poses a real challenge to them, as well as to enforcers.

Because of the passage of new privacy laws in Europe and California, the US appears to be in a moment of national consideration of a federal regime of privacy legislation. That strikes me as very sensible. But I would encourage those of you seeking national preemption to understand that it is not likely to be granted unless it is coupled with a meaningful and effective federal regulatory regime.

Specifically, the FTC would benefit from rule-making authority, coupled with civil penalties in the areas of data security and privacy. Smart, technology-neutral rulemaking would offer transparency and clarity to industry as well. Proving specific financial harm in the privacy space, as our current law often requires, can be extremely difficult. Decoupling monetary relief

---

[14] Press Release, FTC, *Electronic Toy Maker VTech Settles FTC Allegations That it Violated Children's Privacy Law and the FTC Act*, (Jan. 8, 2018), https://www.ftc.gov/news-events/press-releases/2018/01/electronic-toy-maker-vtech-settles-ftc-allegations-it-violated.

[15] FTC Workshop, Fall Technology Series: Smart TV, Dec. 7, 2016, *available at* https://www.ftc.gov/news-events/events-calendar/2016/12/fall-technology-series-smart-tv.

[16] FTC Workshop, Fall Technology Series: Drones, Oct. 13, 2016, *available at* https://www.ftc.gov/news-events/events-calendar/2016/10/fall-technology-series-drones.

[17] FTC Workshop, Connected Cars: Privacy, Security Issues Related to Connected, Automated Vehicles, June 28, 2017, *available at* https://www.ftc.gov/news-events/events-calendar/2017/06/connected-cars-privacy-security-issues-related-connected.

[18] FTC Workshop, Student Privacy and Ed Tech, Dec. 1, 2017, *available at* https://www.ftc.gov/news-events/events-calendar/2017/12/student-privacy-ed-tech.

from redress of demonstrable harm would create more incentive for companies to properly protect privacy. We have models for how to do this in the Children's Online Privacy Protection Act.

Another way for the FTC to be more effective in this area is to elevate our technological expertise into a formal Bureau of Technology. Our cases are more sophisticated than ever and creating, and more critically funding, a body of experts who can assist on our most complex competition and consumer protection cases would be invaluable. We currently put an in-house economist on every single case; we should do the same with a technologist.

We also need more research in the area of privacy and data security—a call echoed by the administration in their proposed privacy goals announced last week. I envision a Bureau of Technology producing scholarship on a host of emerging issues and policy questions in the technology space that impact consumers and competition: IoT security, AI, and data portability to name a few.

And, in the spirit of self-reflection, the FTC is in the midst of a series of public hearings this fall and has invited public comment on a number of topics, including the intersection between privacy, big data and competition and the FTC's remedial authority to deter unfair and deceptive conduct in privacy and data security matters. We are seeking public comment and participation in these hearings and I encourage you all to consider reaching out with your thoughts, in particular your observations of challenges and opportunities in the IoT space.

Thank you again to Forum Global for hosting this annual event and I look forward to further discussion on security and innovation in the IoT space.